УДК 004.8

Пахлебухина В.Г.
студентка 3 курса
факультет «Информационные системы и технологии»
ФГБОУ ВО ПГУТИ
Россия, г. Самара
Пальмов С.В.
к.т.н.
доцент кафедры «Информационные системы и технологии»
ФГБОУ ВО ПГУТИ
Россия, г. Самара
Pakhlebukhina V.G.
3rd year student
Faculty of "Information systems and technologies"
Volga State University of Telecommunications and Informatics,
Russia, Samara
Palmov S.V.
Ph.D. of Engineering Sciences associate
professor of the department
"Information systems and technologies"
Volga State University of Telecommunications and Informatics,
Russia, Samara

ЧТО ТАКОЕ IoT?

Аннотация: Данная статья посвящена такому понятию, как IoT (англ. Internet of Things – Интернет вещей). В ней приведены и изучены области применения, рассмотрены проблемы защиты данных и конфиденциальности в Интернете вещей.

Ключевые слова: IoT, интернет.

WHAT IS THE IoT?

Abstract: This article is devoted to such a concept as IoT (English Internet of Things). The fields of application are presented and studied, the problems of data protection and privacy in the Internet of Things are considered.

Keywords: IoT, Internet.

Постоянное желание человека упростить свою жизнь все быстрее сокращает временной отрезок между фантастикой и обыденностью. Видеосвязь - через смартфон, автомобиль - без водителя, зарядка - беспроводная. В окружающие людей предметы масштабно внедряется Интернет вещей: холодильник, транспорт, уличный фонарь - всем можно управлять по сети. Вот и получается, что не успеем оглянуться, как спустя всего несколько лет, количество предметов, подключённых к IoT-сетям, превысит число мобильников на планете.

Интернет вещей относится к миллиардам физических устройств по всему миру, которые теперь подключены к глобальной паутине, собирают и обмениваются данными. Благодаря дешевым процессорам и беспроводным сетям в элемент IoT можно превратить что угодно - от таблетки до самолета. Практически любой физический объект может быть преобразован в устройство IoT, если он будет подключен к Сети и тем самым контролироваться дистанционно с использованием встроенных датчиков для сбора данных. Девиз IoT: «Все, что может быть подключено к Интернету, будет подключено». [1]

Устройства, подключаемые к Интернету, изобретены давно, но они были не доступны рядовому пользователю из-за высокой цены и, как следствие, низкой популярности. В настоящее время глобальная сеть широко распространена, а большую часть техники производят с различными датчиками, Wi-Fi- и Bluetooth-модулями. Мобильные устройства, при помощи которых можно осуществлять удаленное управления, современного человека.

Первоначально IoT был наиболее интересен для бизнеса и производства, но теперь основное внимание уделяется внедрению интеллектуальных устройств в дома и офисы. По словам аналитиков, наиболее часто используемыми устройствами IoT для предприятий являются интеллектуальные электрические счетчики и коммерческие камеры видеонаблюдения.

IoT - это больше, чем просто удобство для потребителей. Он продолжает развиваться и расширяться. Также Интернет вещей предлагает новые бизнес-модели, которые могут быть использованы в [4]:

- здравоохранении
- промышленности
- торговле
- транспорте
- оказании коммунальных услуг
- умных домах

Рассмотрим перечислено подробнее.

Одно из многих направлений, которое все больше обретает популярность – это медицина, а точнее мониторинг здоровья. Многие люди уже применяют переносные устройства, которые помогают контролировать физические упражнения, сон и другие привычки касательно здоровья, например, датчики физической активности, пульсометры, смарт-градусники и многое другое. И это малая часть того, как IoT влияет на медицину. Устройства мониторинга пациента, электронные записи могут помочь докторам быть информированными о том, как часто и когда их пациенты принимают лекарство, а те, у кого есть проблемы со здоровьем, будут иметь возможность контролировать такие факторы, как давление и уровень сахара, дистанционно.

Следующее направление – промышленность. Датчики сбора данных, встроенные в фабричные машины или складские стеллажи, могут передавать информацию о возникающих проблемах или отслеживать ресурсы в режиме реального времени, что упрощает работу и снижает затраты. Датчики машинного мониторинга диагностируют и прогнозируют ожидаемые проблемы технического обслуживания, расход запасы деталей и даже расставляют приоритеты в расписании обслуживания ремонтного оборудования.

Следующая сфера — это торговля. Как потребители, так и магазины могут воспользоваться IoT. Например, магазины могут использовать Интернет вещей для отслеживания запасов или в целях безопасности, а также для получения информации о наиболее продаваемых товарах

IoT также влияет на транспорт. Вождение будет намного безопаснее. Светофоры смогут корректировать условия движения в реальном времени, например, когда приближается автомобиль скорой помощи. Дорожные датчики будут вносить изменения в ограничение скорости, основанное на погоде и авариях, а также выводить сообщения непосредственно на приборных панелях автомобилей о небезопасных ситуациях. [2]

Также существует возможность применения Интернета вещей в доме, а точнее использование его для удобной регулировки коммунальных услуг**.** Использование бытовой техники с высоким энергопотреблением будет регулироваться на основе динамического изменения цен, чтобы снизить издержки. Термостаты и освещение изучат ваши привычки, чтобы создать оптимальные настройки, основанные на вашей повседневной жизни, например, установят идеальную температуру непосредственно перед тем, как вы придете домой. Эти гаджеты также будут ощущать, когда никто не находится в доме и автоматически отключаться, чтобы уменьшить количество затрат.

IoT генерирует огромное количество данных: от датчиков, прикрепленных к частям машины до слов, с помощью которых можно управлять интеллектуальными колонками. Это означает, что IoT является важным хранилищем больших данных (big data), поскольку позволяет компаниям создавать обширные наборы данных и анализировать их. Следовательно, предоставление производителю огромных объемов данных в режиме реального времени о том, как его продукты ведут себя в реальных ситуациях, может помочь им сделать улучшения в новых товарах намного быстрее, а данные, полученные от датчиков вокруг дорог, могут помочь планировщикам сделать транспортный поток более эффективным.

Но когда все эти датчики собирают данные обо всем, что вы делаете, IoT становится огромной головной болью в разрезе конфиденциальности. К примеру, умный дом: он знает, когда вы проснулись (когда активирована умная кофемашина), и насколько хорошо вы почистили зубы (благодаря вашей умной зубной щетке), какое радио вы слушаете (из-за его прослушивания с помощью умной колонки), какую пищу вы едите (благодаря вашей умной духовке или холодильнику), о чем думают ваши дети (с помощью их умных игрушек), и кто вас посещает и проходит мимо вашего дома (благодаря вашему умному дверному звонку).[3] Не все компании по созданию умных домов, строят свою бизнес-модель вокруг сбора и продажи ваших данных, но некоторые все-таки делают это. И то, что происходит с этими данными, является жизненно важным вопросом конфиденциальности.

Следовательно, безопасность – это одна из самых больших проблем IoT. Защита данных имеет жизненно важное значение для доверия потребителей, но до сих пор показатель безопасности IoT крайне низок. Одна из проблем многих «умных» устройств - отсутствие шифрования передаваемых данных. Ошибки программистов обнаруживаются регулярно, но многие устройства IoT не имеют возможности обновления, поэтому они постоянно подвергаются риску. Хакеры теперь активно нацелены на такие

устройства IoT, как маршрутизаторы и веб-камеры, поскольку отсутствие надежной защиты позволяет им легко осуществлять взлом и организовать гигантские бот-сети.

Также эти недостатки оставляют для хакеров доступ к интеллектуальным домашним устройствам, такие как холодильники, печи и посудомоечные машины. Исследователи обнаружили 100 000 веб-камер, которые были с легкостью взломаны, пока они оставались подключены к Интернету, что позволяло хакерам отслеживать местоположение пользователя, подслушивать разговоры или даже общаться с ним.

Когда стоимость изготовления мобильных устройств станет незначительной, эти проблемы станут более распространенными и неразрешимыми.

IoT преодолевает разрыв между цифровым и физическим миром, а это означает, что взлом устройств может иметь опасные последствия для реального мира. Взлом датчиков, контролирующих температуру на электростанции, управление автомобилем без водителя и т. д может закончиться катастрофой. В настоящее время тема Интернета вещей стала самой распространенной во многих развитых странах. Большинство компаний понимают, что за IoT будущее, и пытаются внедрять эти данные в разработку своих продуктов. В последнее время компании отмечают, что, благодаря этому, поднимается рост продаж. Следовательно, IoT в самое ближайшее время станет главной частью маркетинга каждой компании, целью которых будет являться развитие на рынке труда и сохранение ведущих мест. Но нужно отметить, что IoT - новая технология, которая нуждается в усовершенствовании.

Список использованных источников

1. Интернет вещей. Что это такое и как это работает? [Электронный ресурс] - Режим доступа: https://meduza.io/cards/internet-veschey-chto-eto-takoe-i-kak-eto-rabotaet (дата обращения: 01.05.2018)

2. 8 Ways the 'Internet of Things' Will Impact Your Everyday Life [Электронный ресурс] - Режим доступа: https://www.entrepreneur.com/article/230975 (дата обращения: 01.05.2018)

3. What is the Internet of Things (IoT) [Электронный ресурс] - Режим доступа: https://www.sas.com/en_us/insights/big-data/internet-of-things.html (дата обращения: 01.05.2018)

4. What is the IoT? [Электронный ресурс] - Режим доступа: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (дата обращения: 01.05.2018)